(19) JAPANESE PATENT OFFICE (JP)

(12) KOKAI TOKUHYO PATENT GAZETTE (A)

(11) PATENT APPLICATION PUBLICATION NO. P2002-232420A

(43) Publication Date: August 16, 2002

(51) Int. Cl.[7]:		Identification Codes:	FI		Theme codes (for reference)	
H 04 L	9/32		G 06 F	13/00	630A	5J104
G 06 F	13/00	630	H 04 L	12/28	300A	5K033
H 04 Q	7/38				300Z	5K067
H 04 L	12/28	300		9/00	675A	
			H 04 B	7/26	109M	

Examination Request: Not filed

No. of Claims: 11 (Total of 14 pages: OL)

(21) Filing No.: P2001-23143

(22) Filing Date: January 31, 2001

(71) Applicant: 000003067
TDK Corporation 1-13-1 Nihonbashi, Chuo-ku, Tokyo

(72) Inventor: Masao Tetsuka TDK Corporation 1-13-1 Nihonbashi, Chuo-ku, Tokyo

(74) Agent: 100078031
Koichi Oishi, patent attorney, and 1 other

F Terms (for reference)
5J104 AA07 AA16 EA08 KA02 KA08 NA01 NA02
5K033 AA08 DA17
5K067 AA34 AA35 BB21 DD17 EE02 EE35 EH22 HH36 KK15

(54) Title: WIRELESS COMMUNICATION DEVICE, WIRELESS COMMUNICATION SYSTEM, AND CONNECTION AUTHENTICATION METHOD

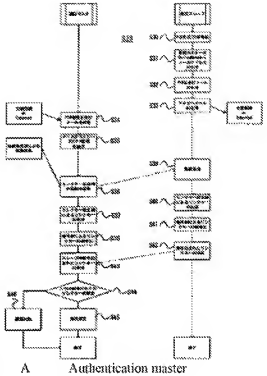
(57) Abstract

Objective

To provide a wireless communication system with improved convenience for the user regarding the connection between the authentication master and authentication slave.

Means to solve

In a wireless communication system comprised of an authentication master and an authentication slave, the connection between the authentication master and the authentication slave is established under the condition that the encrypted information is generated based on at least an encryption key and authentication identification information. The encryption key is generated in the authentication master and is sent wirelessly to the authentication slave. The authentication identification information is generated in the authentication slave and is sent by email to the authentication master. In this way, the convenience is improved since there is no need for the user to enter the authentication identification information.



Key:

A	Authentication master
B	Authentication slave
C	End
S30	Generate PIN/start timing
S31	Generate email address from the device name of the authentication master
S32	Generate an email including PIN
S33	Send the email to the authentication master via public line or Internet
S34	Receive the email including the PIN information via public line or Internet
S35	Extract the PIN number of the authentication slave from the email
S36	Send a random number to the link key generator, Random number is generated by the random number generator
S37	Generate a link key by the link key generator
S38	Encrypt the link key by the encryption unit
S39	Receive the random number
S40	Generate a link key by the link key generator
S41	Encrypt the link key by the encryption unit
S42	Send the encrypted link key
S43	Receive the encrypted link key from the authentication slave
S44	Compare the two encrypted link keys
S45	Successful authentication
S46	Failed authentication

Claims

1. Wireless communication device equipped with a means that acquires the device identification information of another wireless communication device in response to a connection request from said other wireless communication device and generates authentication identification information, a means that generates the email address of said other wireless communication device based on said acquired device identification information, and a means that transmits an email including said authentication identification information to said other wireless communication device by using said email address.

2. Wireless communication device described in Claim 1, characterized by also having a means that generates encrypted information based on at least an encryption key and said authentication identification information upon receiving said encryption key from said other wireless communication device after said email has been sent and a means that wirelessly transmits said encrypted information to said other wireless communication device.

3. Wireless communication device described in Claim 2, characterized by the fact that if the encryption key is not received from said other wireless communication device within a prescribed period of time after said email has been sent, the transmission of said encrypted information is stopped by the means that sends said encrypted information.

4. Wireless communication device described in any of Claims 1-3, characterized by the fact that the means that generates said email address extracts at least part of the aforementioned acquired device identification information and uses that information as the email address.

5. Wireless communication device described in any of Claims 1-3, characterized by the fact that the device also has a management table showing the corresponding relationship between said device identification information and said email address, and the means that generates said email address generates the email address from said device identification information with reference to said management table.

6. Wireless communication device equipped with a means that requests a connection to another wireless communication device, a means that wirelessly sends its own device identification information to said other wireless communication device, a means that generates an encryption key upon receiving an email including the authentication identification information from said other wireless communication device after said device identification information has been sent, and a means that wirelessly sends said encryption key to said other wireless communication device.

7. Wireless communication device described in Claim 6, characterized by also having a means that generates encrypted information based on at least said encryption key and said authentication identification information and a means that compares said generated encrypted

information with said received encrypted information upon receiving the encrypted information from said other wireless device.

8. Wireless communication system comprised of an authentication master and an authentication slave, wherein the connection between the authentication master and the authentication slave is established under the condition that the encrypted information is generated based on at least an encryption key and authentication identification information, characterized by the fact that said encryption key is generated in said authentication master and is sent wirelessly to said authentication slave, and said authentication identification information is generated in said authentication slave and is sent by an email to said authentication master.

9. Wireless communication system described in Claim 8, characterized by the fact that the encryption key is sent to said authentication slave by said authentication master upon receiving said email sent from said authentication slave.

10. Connection authentication method used for establishing a wireless connection between an authentication master and an authentication slave and having the following steps: device identification information is exchanged between said authentication master and authentication slave; said authentication slave generates authentication identification information; said authentication slave generates an email address based on said device identification information of said authentication master; said authentication slave uses said email address to send an email including said authentication identification information to said authentication master; said authentication master generates an encryption key upon receiving said email; said authentication master wirelessly sends said encryption key to said authentication slave; said authentication master and said authentication slave generate encrypted information based on at least said encryption key and said authentication identification information, and the encrypted information generated by said authentication master is compared with the encrypted information generated by said authentication slave.

11. Connection authentication method described in Claim 10, characterized by the fact that said exchange step includes the following sub-steps: said authentication master requests said authentication slave to send device identification information; said authentication slave sends its own device identification information to said authentication master in response to said request; said authentication master sends a connection request to said authentication slave upon receiving the device identification information of said authentication slave; said authentication slave requests said authentication master to send device identification information in response to said connection request; in response, said authentication master sends its own device identification information to said authentication slave.

Detailed explanation of the invention

[0001]

Technical field of the invention

The present invention pertains to a wireless communication device, a wireless communication system, and a connection authentication method. More specifically, the present invention pertains to a wireless communication device, a wireless communication method, and a connection authentication method with improved convenience for the user regarding the connection between the authentication master and authentication slave.

[0002]

Prior art

In recent years, wireless communication systems based on the Bluetooth protocol have attracted a lot of attention as wireless communication systems over short distances. The Bluetooth protocol is an authentication communication protocol and is used at very close ranges. It can set up a low-cost, high-speed wireless communications environment. A frequency of about 2.4 GHz is used for wireless communications based on the Bluetooth protocol, and its radio wave connection range is about 10-100 m.

[0003]

At least two Bluetooth terminals are connected to each other via wireless communication based on the Bluetooth protocol. A prescribed authentication process is carried out during a connection process. In this case, the Bluetooth terminal on the side issuing a connection request is known as the "authentication master," while the Bluetooth terminal on the side receiving the connection request is known as the "authentication slave."

[0004]

Figure 6 is a block diagram schematically illustrating the configuration of a conventional Bluetooth terminal.

[0005]

As shown in Figure 6, the Bluetooth terminal acting as the authentication master and the Bluetooth terminal acting as the authentication slave have the same constituent elements. Both of the Bluetooth terminals have an antenna AT with weak orientation used for transmission/reception. Each terminal has a device controller (CPU) 1 that performs various controls of the device, a baseband link controller 2 that performs link control for baseband, RF unit 3 that performs control during transmission/reception in the RF (radio frequency) range, a

memory 4 storing the PIN (personal identification information) information needed for the authentication procedure, a link key generator 5 that generates a link key for encryption, a program memory 6 that stores the program to execute by CPU 1, a random number generator 7 that generates a random number, an encryption unit 8 that performs encryption, and a PIN input unit 9 used by the user to enter the PIN information.

[0006]

In this case, the PIN information includes numbers, symbols, characters, and the like. It is used as a kind of password for determining in the authentication slave whether the Bluetooth terminal requesting connection (authentication master) is a Bluetooth terminal with connection permission.

[0007]

In the following, the process from the terminal selection to the actual connection using the conventional Bluetooth terminal will be explained.

[0008]

Figure 7 is a flow chart illustrating the process from the terminal selection to the actual connection using the conventional Bluetooth terminal.

[0009]

As shown in Figure 7, first, the authentication master requests the authentication slave to send the device name (S1). In this case, the device name is any name assigned to a specific Bluetooth terminal. It plays an auxiliary role for the ID or Bluetooth address of each Bluetooth terminal. Upon receiving the request, the authentication slave sends its own device name to the authentication master (S2). The authentication master receives the device name (S3). In this case, if there is a plurality of authentication slaves requested to send device names, the authentication master will receive a device name from each of the authentication slaves.

[0010]

Then, the authentication master selects one of them as the connection target based on the device name received from the authentication slave (S4). When the selection of the connection target is completed, an authentication process is carried out between the authentication master and the selected authentication slave (S5). If the authentication is successful in this process, the connection between these two terminals is established. If the authentication fails, the two terminals are disconnected.

[0011]

Figure 8 is a flow chart illustrating the contents in the conventional authentication process (S5).

[0012]

As shown in Figure 8, in the authentication process (S5), first, the authentication master starts the random number generator 7 to generate a random number and sends it to an authentication slave for which the random number is selected (S6). After that, when the user enters the PIN information via PIN input unit 9, a link key is generated by a prescribed algorithm based on the aforementioned random number and the entered PIN information (S7), and the generated link key is encrypted (S8). In this case, the PIN information that should be entered by the user is the same as the PIN information stored in the memory 4 of the authentication slave. If PIN information that is different from the PIN information stored in the memory is entered, the authentication will fail as to be explained below.

[0013]

On the other hand, upon receiving the aforementioned random number (S9), the authentication slave reads out the PIN information stored in memory 4 and generates a link key by a prescribed algorithm based on the received random number and the read PIN information (S10). Then, the authentication slave encrypts the generated link key (S11) and sends the encrypted link key to the authentication master (S12).

[0014]

Upon receiving the encrypted link key from the authentication slave (S13), the authentication master compares the encrypted link key generated in the authentication master and the received encrypted link key (S14). If the comparison result shows that the two link keys are the same, the authentication process (S5) is ended as a successful authentication (S15). If the two link keys are different from each other, the authentication process (S5) is ended as a failed authentication (S16).

[0015]

If the authentication is successful (S15) in the authentication process (S5), a connection is established between the authentication master and the authentication slave. If the authentication fails (S16), the two terminals are disconnected.

[0016]

Problem to be solved by the invention

In the aforementioned conventional authentication process (S5), however, since the user must enter the PIN information from the side of the Bluetooth terminal acting as the authentication master, it is complicated to establish a connection between the authentication master and the authentication slave. In particular, if the Bluetooth terminal acting as the authentication slave is a small terminal, such as a cellular phone, it is very difficult to enter PIN information composed of numbers, symbols, characters, and the like. This adversely affects the convenience for the user.

[0017]

This problem occurs not only when establishing a connection between the aforementioned Bluetooth terminals but also when establishing a connection between various kinds of wireless communication terminals that are connected to each other by confirming the agreement between PIN information or similar information.

[0018]

Consequently, the objective of the present invention is to provide a wireless communication device, a wireless communication system, and a connection authentication method with improved convenience for the user regarding the connection between the authentication master and authentication slave.

[0019]

Means to solve the problem

In order to realize the aforementioned objective, the present invention provides a wireless communication device equipped with a means that acquires the device identification information of another wireless communication device in response to a connection request from said other wireless communication device and generates authentication identification information, a means that generates the email address of said other wireless communication device based on said acquired device identification information, and a means that transmits an email including said authentication identification information to said other wireless communication device by using said email address.

[0020]

According to the present invention, since the authentication identification information is generated internally and is sent by email, said other wireless communication device can share the

authentication identification information by receiving the email. Consequently, there is no need for the user to enter the authentication identification information, which can improve convenience. Also, since the authentication identification information is shared via email, an unauthorized connection to a third party who is not associated with the device identification information and the email address can be prevented so that security can also be improved.

[0021]

In a preferable embodiment of the present invention, the wireless communication device also has a means that generates encrypted information based on at least an encryption key and said authentication identification information upon receiving said encryption key from said other wireless communication device after said email has been sent and a means that wirelessly transmits said encrypted information to said other wireless communication device.

[0022]

In another preferable embodiment of the present invention, if the encryption key is not received from said other wireless communication device within a prescribed period of time after said email has been sent, the transmission of said encrypted information is stopped by the means that sends said encrypted information.

[0023]

According to yet another preferable embodiment of the present invention, even if a third party accesses the authentication identification information improperly, it is very difficult to use the authentication identification information to establish the actual connection so that the security can be further improved.

[0024]

In yet another preferable embodiment of the present invention, said email address extracts at least part of the aforementioned acquired device identification information and uses that information as the email address.

[0025]

In yet another preferable embodiment of the present invention, the device also has a management table showing the corresponding relationship between said device identification information and said email address, and the means that generates said email address generates the email address from said device identification information with reference to said management table.

[0026]

According to yet another preferable embodiment of the present invention, an unauthorized connection established by a third party who does not have the management table can be prevented more effectively so that security can be further improved.

[0027]

In order to realize the aforementioned objective, the present invention also provides a wireless communication device equipped with a means that requests a connection to another wireless communication device, a means that wirelessly sends its own device identification information to said other wireless communication device, a means that generates an encryption key upon receiving an email including the authentication identification information from said other wireless communication device after said device identification information has been sent, and a means that wirelessly sends said encryption key to said other wireless communication device.

[0028]

According to the present invention, since the authentication identification information is received via email, there is no need for the user to enter the authentication identification information, which can improve the convenience.

[0029]

In a preferable embodiment of the present invention, the aforementioned wireless communication device also has a means that generates encrypted information based on at least said encryption key and said authentication identification information and a means that compares said generated encrypted information with said received encrypted information upon receiving the encrypted information from said other wireless device.

[0030]

In order to realize the aforementioned objective, the present invention also provides a wireless communication system comprised of an authentication master and an authentication slave, wherein the connection between the authentication master and the authentication slave is established under the condition that the encrypted information is generated based on at least an encryption key and authentication identification information, characterized by the fact that said encryption key is generated in said authentication master and is sent wirelessly to said

authentication slave, and said authentication identification information is generated in said authentication slave and is sent by an email to said authentication master.

[0031]

According to the present invention, when the authentication identification information is generated in the authentication slave and is sent by email to the authentication server, since the authentication identification information is shared between the authentication master and the authentication slave, there is no need for the user to enter the authentication identification information so that the convenience can be improved.

[0032]

In a preferable embodiment of the present invention, the encryption key is sent to said authentication slave by said authentication master upon receiving said email sent from said authentication slave.

[0033]

In order to realize the aforementioned objective, the present invention also provides a connection authentication method used for establishing a wireless connection between an authentication master and an authentication slave and having the following steps: device identification information is exchanged between said authentication master and authentication slave; said authentication slave generates authentication identification information; said authentication slave generates an email address based on said device identification information of said authentication master; said authentication slave uses said email address to send an email including said authentication identification information to said authentication master; said authentication master generates an encryption key upon receiving said email; said authentication master wirelessly sends said encryption key to said authentication slave; said authentication master and said authentication slave generate encrypted information based on at least said encryption key and said authentication identification information, and the encrypted information generated by said authentication master is compared with the encrypted information generated by said authentication slave.

[0034]

In a preferable embodiment of the present invention, the aforementioned exchange step includes the following sub-steps: said authentication master requests said authentication slave to send device identification information; said authentication slave sends its own device identification information to said authentication master in response to said request; said

authentication master sends a connection request to said authentication slave upon receiving the device identification information of said authentication slave; said authentication slave requests said authentication master to send device identification information in response to said connection request; in response, said authentication master sends its own device identification information to said authentication slave.

[0035]

Embodiment of the invention

In the following, the preferable embodiments of the present invention will be explained in detail with reference to the attached figures.

[0036]

Figure 1 is a block diagram illustrating the configuration of the wireless communication device 10 in a preferable embodiment of the present invention. In this embodiment, the wireless communication device 10 is a Bluetooth terminal. Its constituent elements are represented by the same symbols used for the aforementioned conventional Bluetooth terminal.

[0037]

As shown in Figure 1, the Bluetooth terminal 10 acting as the authentication master and the Bluetooth terminal 10 acting as the authentication slave have the same constituent elements. Both of the Bluetooth terminals 10 have an antenna AT with weak orientation used for transmission/reception. Each terminal has a device controller (CPU) 1 that performs various controls of the device, a baseband link controller 2 that performs link control for baseband, RF unit 3 that performs control during transmission/reception in the RF (radio frequency) range, a link key generator 5 that generates a link key for encryption, a program memory 6 used for storing the program executed by CPU 1, a random number generator 7 that generates a random number as the encryption key, an encryption unit 8 that performs encryption, a public line interface 11 connected to a public line, an email generation controller 12 that generates an email to send via public line interface 11, an email reception controller 13 that receives the email sent via public line interface 11, a PIN generator 14 that automatically generates PIN information as the authentication identification information, a PIN extraction unit 15 that extracts the PIN information from the main text of the received email, and a timer 16.

[0038]

Although both the Bluetooth terminal 10 acting as the authentication master and the Bluetooth terminal 10 acting as the authentication slave each have the aforementioned

constituent elements, it is not required that all of the constituent elements in the Bluetooth terminal 10 acting as the authentication master be exactly the same as those in the Bluetooth terminal 10 acting as the authentication slave. Therefore, they may have different constituent elements. Also, each of the aforementioned constituent elements has the same function in the Bluetooth terminal 10 acting as the authentication master and the Bluetooth terminal 10 acting as the authentication slave. They are not, however, required to have the same hardware. Therefore, it is not required that each of the aforementioned constituent elements have independent hardware. It is possible to realize one or more constituent elements in software by executing programs in the CPU 1.

[0039]

In the following, the process from the selection of the terminal to the actual connection will be explained using the Bluetooth terminals 10 in the aforementioned embodiment.

[0040]

Figure 2 is a flow chart illustrating the process from the selection of the terminal to the actual connection using the Bluetooth terminals 10 in the aforementioned embodiment.

[0041]

As shown in Figure 2, first, the authentication master requests the authentication slave to send its device name as the device identification information (S20). In this case, the device name is a name assigned to each Bluetooth terminal. It plays an auxiliary role for the ID or Bluetooth address of each Bluetooth terminal. In this embodiment, the device name of each Bluetooth terminal 10 is consistent with the email address of the corresponding Bluetooth terminal 10. Upon receiving the request, the authentication slave sends its own device name, that is, the email address to authentication master (S21), and the authentication master receives the device name (S22). In this case, if there is a plurality of authentication slaves requested to send the device name, the authentication master will receive the device name from each of the multiple authentication slaves.

[0042]

Then, the authentication master selects one of them as the connection target based on the user's instructions by using the device name received from the authentication slave (S23). When the selection of the connection target is completed, the authentication master sends a connection request to the authentication slave selected as the connection target (S24). Upon receiving the request (S25), the selected authentication slave requests the authentication master to send the

device name (S26). Upon receiving that request, the authentication master sends its own device name, that is, the email address to the authentication slave (S27). The authentication slave receives the device name (S28).

[0043]

In this way, the exchange of the device name, that is, the email address between the authentication master and the authentication slave is completed. When the exchange of the device name between the authentication master and the authentication slave is completed this way, an authentication process is carried out between the authentication master and the authentication slave (S29). If the authentication is successful in this authentication process, a connection is established between the two terminals. If the authentication fails, the two terminals will be disconnected.

[0044]

Figure 3 is a flow chart illustrating the contents of the authentication process (S29) in this embodiment.

[0045]

As shown in Figure 3, in the authentication process (S29), first, the authentication slave starts PIN generator 14 to generate PIN information (S30). In this case, the PIN information to be generated can be any information including numbers, symbols, characters, and the like. Also, when the PIN information is generated, timer 16 is turned on to start timing.

[0046]

Then, the authentication slave starts the email generation controller 12 to generate the email address of the authentication master based on the device name received from the authentication master in step S28 (S31). In this embodiment, since the email address of the authentication master is consistent with the device name of the authentication master, the email generation controller 12 recognizes the device name as the email address of the authentication master. Also, the authentication slave generates the main text of the email in a prescribed format including the aforementioned generated PIN information by email generation controller 12 (S32).

[0047]

Figure 4 is a diagram illustrating an example of the email main text generated by email generation controller 12.

[0048]

Then, the authentication slave sends the generated email to the authentication master via public line interface 11. In this case, the email address of the receiver is the email address of the authentication master. During that period, the authentication master is in a state waiting for the arrival of the email.

[0049]

Then, when the email sent from the authentication slave is received by the authentication master (S34), the authentication master starts PIN extraction unit 15 to extract the PIN information from the main text of the received email (S35). In this way, the authentication master and the authentication slave share the common PIN information via email.

[0050]

Then, the authentication master starts random number generator 7 to generate a random number as a cipher code and sends it to the authentication slave for which said random number is selected (S36). Then, link key generator 5 is started to generate a link key by a prescribed algorithm based on the aforementioned random number and the extracted PIN information (S37), and the generated link key is encrypted (S38). In the specification of the present invention, the encrypted link key is known as "encrypted information." In this case, the link key is encrypted by an algorithm that is different from the aforementioned algorithm based on the link key and the Bluetooth address of the authentication master. Also, the Bluetooth address is an identifier provided to each Bluetooth device. It is shared between the authentication master and the authentication slave in the stage before the authentication process (S29) is carried out.

[0051]

During that period, the authentication slave is waiting to receive the random number from the authentication master. If the time counted by timer 16 exceeds a prescribed value, the CPU 1 in the authentication slave will cancel the waiting state and forcibly end the authentication process (S29) as a failed authentication. In this case, the aforementioned prescribed value is set in consideration of the time needed for the arrival of the email. It is preferred to set it to about 1-2 min. If it is set too short, a slight delay in the arrival of the email will result in a failed authentication, which will adversely affect the convenience. If the time is set too long, security problems tend to occur.

[0052]

On the other hand, if the authentication slave receives the aforementioned random number before the time counted by timer 16 exceeds the aforementioned prescribed value (S39), the authentication slave starts link key generator 5 to generate a link key by a prescribed algorithm based on the received random number and the PIN information generated by PIN generator 14 (S40). The authentication slave also starts encryption unit 8 to encrypt the generated link key (S41) and sends the encrypted link key to the authentication master (S42). As described above, the link key is encrypted by an algorithm different from the aforementioned algorithm based on the link key and the Bluetooth address of the authentication master.

[0053]

Upon receiving the encrypted link key from the authentication slave (S43), the authentication master compares the encrypted link key generated in the authentication master with the received encrypted link key (S44). If the comparison result shows that the two link keys are the same, the authentication process (S29) is ended as a successful authentication (S45). If the two link keys are different from each other, the authentication process (S29) is ended as a failed authentication (S46).

[0054]

If the authentication is successful (S45) in the authentication process (S29), a connection is established between the authentication master and the authentication slave. If the authentication fails (S46), the two terminals are disconnected.

[0055]

As described above, according to this embodiment, since the PIN information is generated automatically in the authentication slave and is sent by email to the authentication master, there is no need for the user to enter the PIN information in order to establish the connection. The convenience can be improved. Also, since the authentication master and the authentication slave share the PIN information via email, an unauthorized connection to a third party who is not associated with the device identification information and the email address (consistent in this embodiment) can be prevented so that security can also be improved.

[0056]

Also, according to this embodiment, since the timer 16 is used to restrict the time from generation of PIN (S30) to reception of the random number (S39), the authentication process (S29) can be ended automatically when the PIN information cannot be shared due to non-arrival

of the email. Also, even if a third party accesses the PIN information improperly, it is very difficult to use that information to establish an actual connection so that security can be further improved.

[0057]

In the following, another preferable embodiment of the present invention will be explained.

[0058]

Figure 5 is a block diagram illustrating the configuration of the wireless communication device 20 in the said other preferable embodiment of the present invention. In this embodiment, the wireless communication device 20 is also a Bluetooth terminal.

[0059]

As shown in Figure 5, the difference in the Bluetooth terminal 20 in this embodiment is that memory 4 is added to Bluetooth terminal 10 in the aforementioned embodiment. Memory 4 is a nonvolatile memory that can be written electrically, such as EEPROM. In this embodiment, if it is required that the device name be consistent with the email address, a management table indicating the corresponding relationship between the device name of each Bluetooth terminal 20 and the email address of the corresponding Bluetooth terminal is pre-stored in said memory 4. Consequently, it is necessary to register the device name and email address of a Bluetooth terminal 20 expected to be connected in the memory 4 of each Bluetooth terminal 20 to form the management table.

[0060]

The process of establishing a connection between the authentication master and the authentication slave in this embodiment is the same as that in the aforementioned embodiment except for the operation in step S31 shown in Figure 3. In this embodiment, in step S31, the authentication slave generates the email address of the authentication master with reference to the management table stored in memory 4 based on the device name received from the authentication master in step S28.

[0061]

As described above, according to this embodiment, the management table showing the corresponding relationships between the device names of each Bluetooth terminal 20 and the email addresses of those Bluetooth terminal is stored in memory 4, and the authentication slave

generates the email address of the authentication master with reference to that table. Therefore, in addition to the effect realized by the aforementioned embodiment, an unauthorized connection by a third party who does not have this management table can be effectively prevented.

[0062]

The present invention is not limited to the aforementioned embodiments. Various modifications can be made within the range of the present invention described in the claims and they are also included within the scope of the present invention.

[0063]

For example, the device name and email address of each Bluetooth terminal 10 in the aforementioned embodiments are consistent with each other. They are not, however, necessarily exactly the same. It is also possible for a part of the email address to be consistent with the device name. For example, if the email address of a certain Bluetooth terminal 10 is 123456@xxxxx.ne.jp, the device name of that terminal can be 123456. In this case, the part of "@xxxxx.ne.jp" should be common for the Bluetooth terminals 10 expected to be connected. The email generation controller 12 can generate the email address of the authentication master by adding "@xxxxx.ne.jp" to the received device name "123456" in step S31.

[0064]

Similarly, it is also possible to use information formed by varying the email address based on a prescribed algorithm as the device name of the Bluetooth terminal 10. In this case, if the aforementioned algorithm is shared by Bluetooth terminals 10 expected to be connected, an unauthorized connection by a third party who does not know the algorithm can be prevented more effectively. In this case, email generation controller 12 can generate the email address of the authentication master by resuming the email address from the received device name in step S31.

[0065]

It is also possible to use the telephone number corresponding to the email address as the device name of Bluetooth terminal 10. In this case, email generation controller 12 can obtain the email address from the email service provider based on the telephone number or send the PIN information to the email service provider and can request that the email service provider send an email to the authentication master in step S31.

[0066]

Also, in each of the embodiments described above, the wireless communication device is the Bluetooth terminal 10 (20). The device, however, is not limited to a Bluetooth terminal as long as the connection is established by the aforementioned procedure. Examples of devices to which the present invention is applicable include PC's, PDA's (personal digital assistants), workstations, routers, printers, headsets, digital cameras, hard disk devices, removable disk devices, VTR's, TV's, ac units (air-conditioners), refrigerators, video recording/playback devices (tape recorders, IC recorders, and the like), remote controls, automobiles, vending machines, microwaves, telephones, and the like.

[0067]

In each of the embodiments described above, PIN information is used as the authentication identification information. In the present invention, however, the authentication identification information is not limited to PIN information. It is also possible to use other information as long as it can establish the connection by being shared between the authentication master and the authentication slave.

[0068]

In each of the embodiments descried above, the device name is used as the device identification information. In the present invention, however, the device identification information is not limited to the device name. It is also possible to use other information as long as it can be used to identify each device.

[0069]

In each of the embodiments described above, a random number is used as the cipher code. In the present invention, the cipher code is not limited to a random number. It is also possible to use other information as long as it can be used to encrypt the authentication identification information (PIN information).

[0070]

In each of the embodiments described above, the encrypted link key is used as the encrypted information. In the present invention, however, the encrypted information is not limited to the link key. It is also possible to use other information as long as it is generated based on at least the cipher code (random number) and authentication identification information (PIN information).

[0071]

In each of the embodiments described above, the PIN generator 14 is used to generate PIN information. It is also possible to generate the information by using the random number generator 7 instead of the PIN generator 14. That is, on the side of the authentication master, the random number generated by the random number generator 7 is used as the random number to send to the authentication slave in step S36. On the side of the authentication slave, the random number generated by the random number generator 7 is used as the PIN information to send to the authentication master in step S33. In this case, the PIN generator 14 can be omitted.

[0072]

Also, in the present invention, the means does not necessarily mean physical means. It includes the case where the function of each means is realized by software. It is also possible to realize the function of one means by two or more physical means or to realize the functions of two or more means by one physical means.

[0073]

Effects of the invention

As explained above, the present invention provides a wireless communication system, a wireless communication method, and a connection authentication method with improved convenience for the user regarding the connection between the authentication master and authentication slave.

Brief description of figures

Figure 1 is a block diagram schematically illustrating the configuration of the Bluetooth terminal 10 in a preferable embodiment of the present invention.

Figure 2 is a flow chart illustrating the process from the selection of the terminal to the actual connection using the Bluetooth terminals 10 in the aforementioned embodiment.

Figure 3 is a flow chart illustrating the contents of the authentication process (S29) in a preferable embodiment of the present invention.

Figure 4 is a diagram illustrating an example of the main text of the email generated by email generation controller 12.

Figure 5 is a block diagram schematically illustrating the configuration of the Bluetooth terminal 20 in another preferable embodiment of the present invention.

Figure 6 is a block diagram schematically illustrating the configuration of a conventional Bluetooth terminal.

Figure 7 is a flow chart illustrating the process from the selection of the terminal to the actual connection using the conventional Bluetooth terminal.

Figure 8 is a flow chart illustrating the contents of the conventional authentication process (S5).

Explanation of symbols

1 CPU
2 Baseband link controller
3 RF unit
4 Memory
5 Link key generator
6 Program memory
7 Random number generator
8 Encryption unit
9 PIN input unit
10 Wireless communication device (Bluetooth terminal)
11 Public line interface
12 Email generation controller
13 Email reception controller
14 PIN generator
15 PIN extraction unit
16 Timer
20 Wireless communication device (Bluetooth terminal)

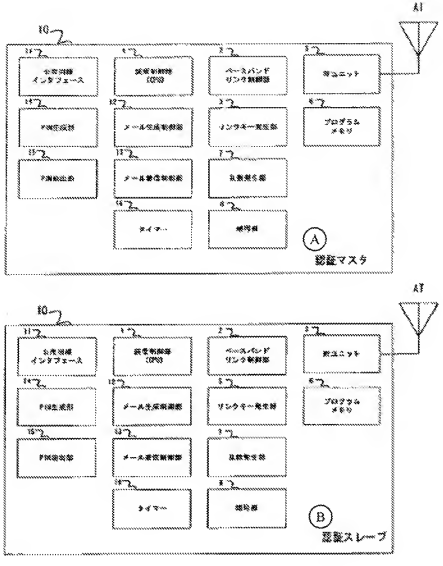


Figure 1

Key: A Authentication master
B Authentication slave
1 CPU
2 Baseband link controller
3 RF unit
5 Link key generator
6 Program memory
7 Random number generator
8 Encryption unit
9 PIN input unit
11 Public line interface

12 Email generation controller
13 Email reception controller
14 PIN generator
15 PIN extraction unit
16 Timer

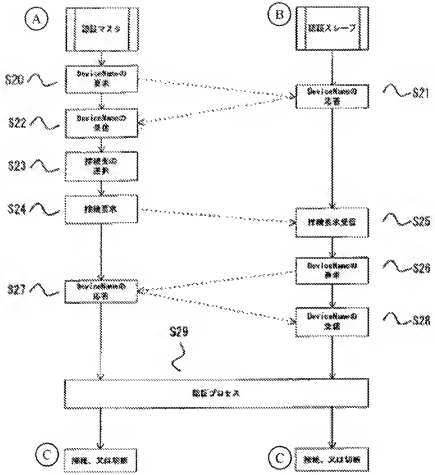


Figure 2

Key: A Authentication master
B Authentication slave
C Connect or disconnect
S20 Request for device name
S21 Response of device name
S22 Receive device name
S23 Select connection target
S24 Connection request
S25 Receive connection request
S26 Request for device name

S27 Response of device name
S28 Receive device name
S29 Authentication process

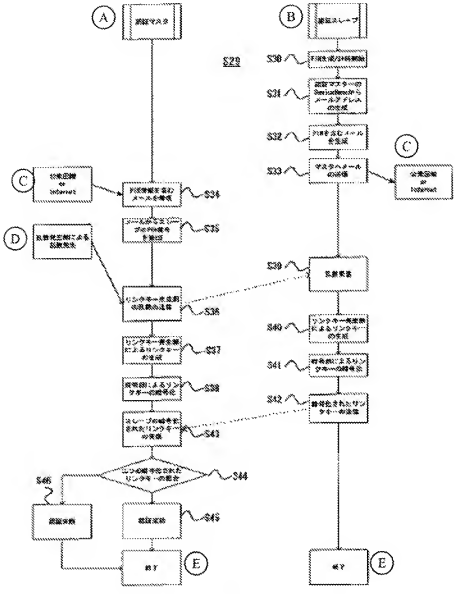


Figure 3

Key: A Authentication master
B Authentication slave
C Public line or Internet
D Random number is generated by the random number generator
E End
S30 Generate PIN/start timing
S31 Generate email address from the device name of the authentication master

S32 Generate an email including PIN
S33 Send the email to the authentication master
S34 Receive the email including the PIN information via public line or Internet
S35 Extract the PIN number of the authentication slave from the email
S36 Send a random number to the link key generator
S37 Generate a link key by the link key generator
S38 Encrypt the link key by the encryption unit
S39 Receive the random number
S40 Generate a link key by the link key generator
S41 Encrypt the link key by the encryption unit
S42 Send the encrypted link key
S43 Receive the encrypted link key from the authentication slave
S44 Compare the two encrypted link keys
S45 Successful authentication
S46 Failed authentication

To: xxxx@yyyy.ne.jp
From: tttt@ssss.ne.jp
Sub: Bluetooth Connect Info
PIN: "123456"
Date: yyyy:mm:dd hh:mm:ss

Figure 4

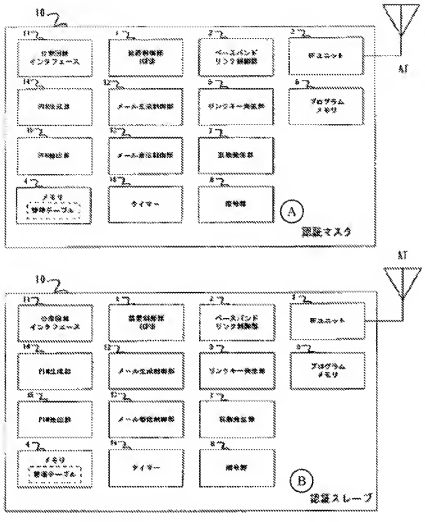


Figure 5

Key: A Authentication master
B Authentication slave
1 CPU
2 Baseband link controller
3 RF unit
4 Memory
Management table
5 Link key generator
6 Program memory
7 Random number generator
8 Encryption unit
9 PIN input unit
11 Public line interface
12 Email generation controller

13 Email reception controller
14 PIN generator
15 PIN extraction unit
16 Timer

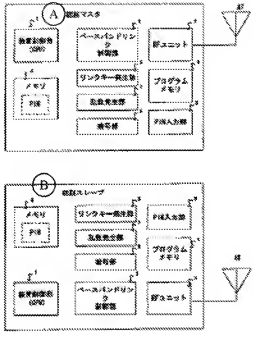


Figure 6

Key: A Authentication master
B Authentication slave
1 Device controller (CPU)
2 Baseband link controller
3 RF unit
4 Memory
5 Link key generator
6 Program memory
7 Random number generator
8 Encryption unit
9 PIN input unit

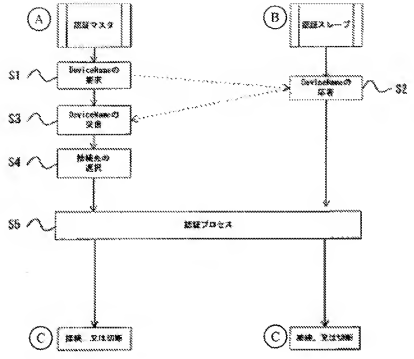


Figure 7

Key:
- A Authentication master
- B Authentication slave
- C Connect or disconnect
- S1 Request device name
- S2 Response of device name
- S3 Receive device name
- S4 Select connection target
- S5 Authentication process

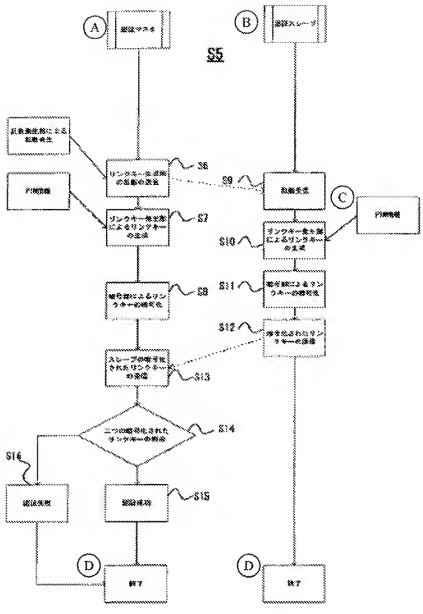


Figure 8

Key: A Authentication master
B Authentication slave
C PIN information
D End
S6 Send a random number for generating link key
S7 Generate a link key by the link key generator
S8 Encrypt the link key by the encryption unit
S9 Receive the random number
S10 Generate a link key by the link key generator

S11 Encrypt the link key by the encryption unit
S12 Send the encrypted link key
S13 Receive the encrypted link key from the authentication slave
S14 Compare the two encrypted link keys
S15 Successful authentication
S16 Failed authentication

Continued from the first page

(51) Int. Cl.[7]:	Identification Codes	FI	Theme Codes (for reference)
H 04 Q 7/10		H 04 L 9/00	673B
7/20		H 04 Q 7/02	Z